# Optimal entanglement witnesses based on local orthogonal observables

Cheng-Jie Zhang,* Yong-Sheng Zhang,† Shun Zhang, and Guang-Can Guo
*Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China*

We show that the entanglement witnesses based on local orthogonal observables which are introduced in [S. Yu and N.-L. Liu, Phys. Rev. Lett. **95**, 150504 (2005)] and [O. Gühne, M. Mechler, G. Tóth and P. Adam, Phys. Rev. A **74**, 010301 (R) (2006)] in linear and nonlinear forms can be optimized, respectively. As applications, we calculate the optimal nonlinear witnesses of pure bipartite states and show a lower bound on the I-concurrence of bipartite higher dimensional systems with our method.

PACS numbers: 03.67.Mn, 03.65.Ta, 03.65.Ud

arXiv:0705.1832v3 [quant-ph] 2 Aug 2007

## I. INTRODUCTION

Entanglement is one of the most fascinating features of quantum mechanics, which has recently been recognized as a basic resource in quantum information processing such as teleportation, dense coding and quantum key distribution [1, 2]. Thus, it becomes particularly important to detect and quantify entanglement [3]. Despite a great deal of effort in the past years, lots of things are still unclear to us in this field (see the reviews [4, 5, 6] and references therein). Nevertheless, on the one hand, several sufficient conditions for detection of entanglement have been found, such as the famous Peres-Horodecki positive partial transpose (PPT) criterion [7, 8], realignment criterion [9], entanglement witnesses (EWs) [10], local uncertainty relations (LURs) [11, 12], Bell type inequalities[13, 14, 15], etc. PPT criterion is necessary and sufficient for $2\times 2$ and $2\times 3$ systems, but only necessary for higher dimensional cases [8]. It is believed that realignment criterion complements PPT criterion since it can detect many entangled states which PPT criterion cannot detect. More easier way to detect entanglement experimentally is using EWs, which have recently been generalized to nonlinear EWs [16, 17]. On the other hand, a considerable amount of effort on quantification of entanglement has also been made. For instance, Wootters has analytically derived a perfect measure of 2 qubits [18], which is so-called *concurrence*. Furthermore, generalized concurrence in bipartite higher dimensional cases [19, 20], such as I-concurrence [20], has been pointed out as well. Unfortunately, the I-concurrence of mixed states is given as a convex roof for all possible ensemble realization. Therefore, it is generally difficult to be calculated. Lately, lower bounds on I-concurrence have attracted much interest [21, 22, 23, 24], which are relatively easier than I-concurrence itself to get.

Recently, Yu and Liu have introduced an entanglement witness [Eq. (3)] based on local orthogonal observables (LOOs) in Ref. [25]. Moreover, Gühne *et al.* have generalized the witness to the nonlinear form [Eq. (4)] via local uncertainty relations [26]. Both of the witnesses have a common property that each set of LOOs in the witnesses can be replaced by any other complete set of LOOs, thus one does not know which set of LOOs is the best one for the witnesses. Actually, the witnesses using different set of LOOs can obtain distinct results. For example, the Bell state $(|00\rangle + |11\rangle)/\sqrt{2}$ can be detected as entangled states by the liner witness under the set of LOOs: $\{\sigma_x, \sigma_y, \sigma_z, I\}^A/\sqrt{2}$, $\{\sigma_x, -\sigma_y, \sigma_z, I\}^B/\sqrt{2}$, but cannot be detected under the LOOs: $\{\sigma_x, \sigma_y, \sigma_z, I\}^A/\sqrt{2}$, $\{\sigma_x, \sigma_y, \sigma_z, I\}^B/\sqrt{2}$. Therefore, it is necessary to investigate the optimal case. In this paper, the optimal witnesses for the linear and nonlinear forms will be presented. As applications, we will calculate the optimal witnesses of pure bipartite states and show a lower bound on the I-concurrence of bipartite higher dimensional systems.

The paper is organized as follows: Sec. II presents the optimal witnesses of linear and nonlinear forms, which are constructed by LOOs. In Sec. III we calculate the optimal nonlinear witnesses of pure bipartite states based on our method. Moreover, we obtain a lower bound of I-concurrence in bipartite systems. Sec. IV discusses what happens if the dimensions of the subsystems A and B are not the same.

## II. OPTIMAL WITNESSES BASED ON LOOS

For convenience, we consider a $d\times d$ bipartite system, just as Refs. [25, 26] did ( in Sec. IV we will discuss the situation when dimensions of subsystems A and B are not the same). Each subsystem has a complete set of local orthogonal bases $\{G_k^A\}$ and $\{G_k^B\}$, which are so-called LOOs. Such a basis consists of $d^2$ observables and satisfies:

$$\mathrm{Tr}(G_k^A G_l^A) = \mathrm{Tr}(G_k^B G_l^B) = \delta_{kl}. \tag{1}$$

Any other complete set of LOOs relate to the original one by an orthogonal $d^2\times d^2$ real matrix, i.e.,

$$\widetilde{G_k^A} = \sum_l O_{kl} G_l^A,\ \widetilde{G_k^B} = \sum_l O'_{kl} G_l^B, \tag{2}$$

*Electronic address: zhangcj@mail.ustc.edu.cn
†Electronic address: yshzhang@ustc.edu.cn

where $OO^T = O^TO = O'O'^T = O'^TO' = I$.

In Ref. [25], a linear witness was introduced as follows (for convenience, the witness has been written in an equivalent form introduced in [26]),

$$\mathcal{W} = 1 - \sum_k G_k^A \otimes G_k^B, \tag{3}$$

where $\{G_k^A\}$ and $\{G_k^B\}$ are arbitrary complete sets of LOOs for subsystems A and B. Later, Ref. [26] provided a nonlinear form,

$$\mathcal{F}(\rho) = 1 - \sum_k \langle G_k^A \otimes G_k^B\rangle - \frac{1}{2}\sum_k \langle G_k^A \otimes I - I \otimes G_k^B\rangle^2. \tag{4}$$

For every separable state $\rho$, it must satisfy that $\mathrm{Tr}\mathcal{W}\rho \geq 0$ and $\mathcal{F}(\rho) \geq 0$. Conversely, if any state violates one of the two inequalities, it is entangled indeed.

In Refs. [25, 26], there is a little mention involving that how to choose a set of LOOs so that $\mathrm{Tr}\mathcal{W}\rho$ or $\mathcal{F}(\rho)$ gets its minimum, and obviously the minimum means a optimal one, since one can obtain distinct results by using different sets of LOOs. Consider the simple example $|\psi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ introduced in Sec. I. Under the set of LOOs $\{\sigma_x, \sigma_y, \sigma_z, I\}^A/\sqrt{2}$, $\{\sigma_x, \sigma_y, \sigma_z, I\}^B/\sqrt{2}$, $\mathrm{Tr}(\mathcal{W}|\psi^+\rangle\langle\psi^+|) = 0$ and $\mathcal{F}(|\psi^+\rangle\langle\psi^+|) = 0$, with which one cannot conclude that $|\psi^+\rangle$ is entangled. However, under the set of LOOs $\{\sigma_x, \sigma_y, \sigma_z, I\}^A/\sqrt{2}$, $\{\sigma_x, -\sigma_y, \sigma_z, I\}^B/\sqrt{2}$, $\mathrm{Tr}(\mathcal{W}|\psi^+\rangle\langle\psi^+|) = -1$ and $\mathcal{F}(|\psi^+\rangle\langle\psi^+|) = -1$. It suggests that $|\psi^+\rangle$ has entanglement. Therefore, it is meaningful to obtain the minimal one. In the following, we will show that the minimum is invariant under local unitary (LU) transformations, and obtain an analytical formula of the minimum.

*Lemma 1.* For a given state $\rho$, the minimum of $\mathrm{Tr}\mathcal{W}\rho$ $[\mathcal{F}(\rho)]$ is LU invariant.

*Proof.–* (Reductio ad absurdum) For a given state $\rho$, suppose that under the set of LOOs $\{M_k^A\}$, $\{M_k^B\}$ $\mathrm{Tr}\mathcal{W}\rho$ $[\mathcal{F}(\rho)]$ gets its minimum $L_1$. We operate an arbitrary LU transformation to $\rho$, i.e., $\rho' = U_A \otimes U_B \rho U_A^\dagger \otimes U_B^\dagger$. For the state $\rho'$, suppose that under the set of LOOs $\{\widetilde{M_k^A}\}$, $\{\widetilde{M_k^B}\}$ $\mathrm{Tr}\mathcal{W}\rho$ $[\mathcal{F}(\rho)]$ gets its minimum $L_2$.

Case i. $L_1 > L_2$. For the state $\rho$, under the set of LOOs $\{U_A^\dagger \widetilde{M_k^A} U_A\}$, $\{U_B^\dagger \widetilde{M_k^B} U_B\}$, $\mathrm{Tr}\mathcal{W}\rho$ $[\mathcal{F}(\rho)]$ is equal to $L_2$. It is a contradiction to that $L_1$ is the minimum of $\mathrm{Tr}\mathcal{W}\rho$ $[\mathcal{F}(\rho)]$.

Case ii. $L_1 < L_2$. For the state $\rho'$, under the set of LOOs $\{U_A M_k^A U_A^\dagger\}$, $\{U_B M_k^B U_B^\dagger\}$, $\mathrm{Tr}\mathcal{W}\rho'$ $[\mathcal{F}(\rho')]$ is equal to $L_1$. It is a contradiction to that $L_2$ is the minimum of $\mathrm{Tr}\mathcal{W}\rho'$ $[\mathcal{F}(\rho')]$.

In a word, if $L_1 \neq L_2$, a contradiction is derived immediately. Therefore, $L_1 = L_2$ always holds and the minimum of $\mathrm{Tr}\mathcal{W}\rho$ $[\mathcal{F}(\rho)]$ is LU invariant. □

*Remark.–* From an experimental point of view, it is valuable for the minimum to satisfy LU invariant condition, since a shared spatial reference frame is no longer needed when one makes a measure of the minimum [27].

*Theorem 1.* The minimum of $\mathrm{Tr}\mathcal{W}\rho$ is equal to $1 - \sum_k \sigma_k(\mu)$, where $\sigma_k(\mu)$ stands for the $k$th singular value of real matrix $\mu$ which is defined as $\mu_{lm} = \mathrm{Tr}(\rho G_l^A \otimes G_m^B)$.

*Proof.–* Before embarking on our proof, it is worth noticing that a similar result of Theorem 1 has also been pointed out in [25]. However, for a convenience to understand Theorem 2, we insist on providing a complete proof. For a given state $\rho$, we choose an arbitrary complete set of LOOs $\{G_k^A\}$, $\{G_k^B\}$. Define that

$$\mu_{lm} = \mathrm{Tr}(\rho G_l^A \otimes G_m^B), \tag{5}$$

and the density matrix can be written as:

$$\rho = \sum_{l,m} \mu_{lm} G_l^A \otimes G_m^B. \tag{6}$$

According to Eq. (2), any other complete set of LOOs $\{\widetilde{G_k^A}\}$, $\{\widetilde{G_k^B}\}$ can be written as $\widetilde{G_k^A} = \sum_l U_{kl} G_l^A$, $\widetilde{G_k^B} = \sum_m V_{km} G_m^B$, where $U$ and $V$ are $d^2 \times d^2$ real orthogonal matrices, i.e. $UU^T = U^TU = VV^T = V^TV = I$. Therefore,

$$\begin{aligned}
\mathrm{minTr}(\mathcal{W}\rho) &= 1 - \max \sum_k \langle \widetilde{G_k^A} \otimes \widetilde{G_k^B}\rangle \\
&= 1 - \max \sum_k \sum_{lm} U_{kl} V_{km} \langle G_l^A \otimes G_m^B\rangle \\
&= 1 - \max \sum_k \sum_{lm} U_{kl} V_{km} \mu_{lm} \\
&= 1 - \max \sum_k [U\mu V^T]_{kk} \\
&= 1 - \mathrm{maxTr}(U\mu V^T).
\end{aligned} \tag{7}$$

Moreover,

$$\mathrm{maxTr}(U\mu V^T) = \mathrm{maxTr}(\mu V^T U) = \sum_k \sigma_k(\mu), \tag{8}$$

where we have used the following theorem [28]:

*Let $A \in M_n$ be a given matrix, and let $A = V\Sigma W^\dagger$ be a singular value decomposition of $A$. Then the problem $max\{Re\ trAU : U \in M_n\ is\ unitary\}$ has the solution $U = WV^\dagger$, and the value of the maximum is $\sigma_1(A) + \cdots + \sigma_n(A)$, where $\{\sigma_i(A)\}$ is the set of singular values of $A$.*

Notice that $\mu$ is a real matrix and its singular value decomposition can be written as $\mu = \mathcal{U}^T\Sigma\mathcal{V}$, where $\mathcal{U}$, $\mathcal{V}$ are real orthogonal matrices and $\Sigma = diag\{\sigma_1(\mu), \sigma_2(\mu), \cdots, \sigma_{d^2}(\mu)\}$. When $U = \mathcal{U}$ and $V = \mathcal{V}$, $\mathrm{Tr}(U\mu V^T)$ gets its maximum $\sum_k \sigma_k(\mu)$. In other words, under the new complete set of LOOs $\{\mathcal{G}_k^A\}$, $\{\mathcal{G}_k^B\}$, where $\mathcal{G}_k^A = \sum_l \mathcal{U}_{kl} G_l^A$, $\mathcal{G}_k^B = \sum_m \mathcal{V}_{km} G_m^B$, $\mathcal{W} = 1 - \sum_k \mathcal{G}_k^A \otimes \mathcal{G}_k^B$, $\mathrm{Tr}\mathcal{W}\rho$ gets its minimum $1 - \sum_k \sigma_k(\mu)$. □

*Remark.–* In fact, it is equivalent to the realignment criterion when $\mathrm{Tr}\mathcal{W}\rho$ gets its minimum [25]. Note that under the new complete set of LOOs $\{\mathcal{G}_k^A\}$, $\{\mathcal{G}_k^B\}$, the

density matrix can be written in its operator-Schmidt decomposition form [29]:

$$\rho = \sum_k \sigma_k(\mu)\mathcal{G}_k^A \otimes \mathcal{G}_k^B. \quad (9)$$

The realignment criterion states that if $\rho$ is separable the sum of all $\sigma_k(\mu)$ is smaller than 1. It is equivalent to $\min \mathrm{Tr}\mathcal{W}\rho \geq 0$. Hence, it is concluded that any entangled state detected by a witness of Eq. (3) must violate the realignment criterion.

*Example.–* Let us consider a noisy singlet state introduced in Ref. [26], $\rho = p|\psi_s\rangle\langle\psi_s| + (1-p)\rho_{sep}$, where $|\psi_s\rangle$ stands for the singlet state $(|01\rangle - |10\rangle)/\sqrt{2}$ and the separable noise is $\rho_{sep} = 2/3|00\rangle\langle 00| + 1/3|01\rangle\langle 01|$. Actually, the state is entangled for any $p > 0$ [26]. Under the complete set of LOOs $\{-\sigma_x, -\sigma_y, -\sigma_z, I\}^A/\sqrt{2}$, $\{\sigma_x, \sigma_y, \sigma_z, I\}^B/\sqrt{2}$, the witness of Eq. (3) can detect the entanglement for all $p > 0.4$. However, the optimal witness using Theorem 1 can detect the entanglement for all $p > 0.292$, which is equivalent to the realignment criterion.

*Theorem 2.* The minimum of $\mathcal{F}(\rho)$ is equal to $1 - \sum_k \sigma_k(\tau) - (\mathrm{Tr}\rho_A^2 + \mathrm{Tr}\rho_B^2)/2$, where $\sigma_k(\tau)$ stands for the $k$th singular value of matrix $\tau$ defined as $\tau_{lm} = \langle G_l^A \otimes G_m^B\rangle - \langle G_l^A \otimes I\rangle\langle I \otimes G_m^B\rangle$.

*Proof.–* For a given state $\rho$, we choose an arbitrary complete sets of LOOs $\{G_k^A\}, \{G_k^B\}$, and calculate the real matrix $\tau$ according to the definition:

$$\tau_{lm} = \langle G_l^A \otimes G_m^B\rangle - \langle G_l^A \otimes I\rangle\langle I \otimes G_m^B\rangle. \quad (10)$$

Similarly to Theorem 1, any other complete set of LOOs $\{\widetilde{G_k^A}\}$, $\{\widetilde{G_k^B}\}$ can be written as $\widetilde{G_k^A} = \sum_l U_{kl}G_l^A$, $\widetilde{G_k^B} = \sum_m V_{km}G_m^B$, where $U$ and $V$ are $d^2 \times d^2$ real orthogonal matrices, i.e. $UU^T = U^TU = VV^T = V^TV = I$. Therefore,

$$\begin{aligned} &\min[1 - \sum_k \langle \widetilde{G_k^A} \otimes \widetilde{G_k^B}\rangle - \frac{1}{2}\sum_k \langle \widetilde{G_k^A} \otimes I - I \otimes \widetilde{G_k^B}\rangle^2] \\ =\ & 1 - \max[\sum_k \langle \widetilde{G_k^A} \otimes \widetilde{G_k^B}\rangle + \frac{1}{2}\sum_k \langle \widetilde{G_k^A} \otimes I - I \otimes \widetilde{G_k^B}\rangle^2]. \end{aligned}$$

Moreover,

$$\begin{aligned} &\sum_k \langle \widetilde{G_k^A} \otimes I - I \otimes \widetilde{G_k^B}\rangle^2 \\ =\ & \sum_k [\langle \widetilde{G_k^A} \otimes I\rangle^2 + \langle I \otimes \widetilde{G_k^B}\rangle^2 - 2\langle \widetilde{G_k^A} \otimes I\rangle\langle I \otimes \widetilde{G_k^B}\rangle], \end{aligned}$$

where $\sum_k \langle \widetilde{G_k^A} \otimes I\rangle^2$ and $\sum_k \langle I \otimes \widetilde{G_k^B}\rangle^2$ are invariant under LOOs transformations, i.e.,

$$\begin{aligned} \sum_k \langle \widetilde{G_k^A} \otimes I\rangle^2 &= \sum_k \sum_{ll'} U_{kl}U_{kl'} \langle G_l^A \otimes I\rangle\langle G_{l'}^A \otimes I\rangle \\ &= \sum_{ll'} [U^TU]_{ll'} \langle G_l^A \otimes I\rangle\langle G_{l'}^A \otimes I\rangle \\ &= \sum_l \langle G_l^A \otimes I\rangle^2 \\ &= \mathrm{Tr}\rho_A^2, \end{aligned}$$

where $\rho_A$ is the reduced density matrix after tracing over subsystem B. Without loss of generality, substituting Eq. (11) into $\sum_l \langle G_l^A \otimes I\rangle^2$, one can obtain the final result $\mathrm{Tr}\rho_A^2$. Similarly, $\sum_k \langle I \otimes \widetilde{G_k^B}\rangle^2 = \sum_l \langle I \otimes G_l^B\rangle^2 = \mathrm{Tr}\rho_B^2$ holds.

$$G_k^A = \begin{cases} \frac{1}{\sqrt{2}}(|m\rangle\langle n| + |n\rangle\langle m|) & 1 \leq m < n \leq d, \\ \frac{1}{\sqrt{2}}(i|m\rangle\langle n| - i|n\rangle\langle m|) & 1 \leq m < n \leq d, \\ |m\rangle\langle m| & 1 \leq m \leq d. \end{cases} \quad (11)$$

$$G_k^B = (G_k^A)^T, \quad (12)$$

where $\{|m\rangle_A\}$ and $\{|m\rangle_B\}$ are the standard complete bases. Thus,

$$\begin{aligned} &\max[\sum_k \langle \widetilde{G_k^A} \otimes \widetilde{G_k^B}\rangle + \frac{1}{2}\sum_k \langle \widetilde{G_k^A} \otimes I - I \otimes \widetilde{G_k^B}\rangle^2] \\ =\ & \frac{1}{2}\sum_k [\langle \widetilde{G_k^A} \otimes I\rangle^2 + \langle I \otimes \widetilde{G_k^B}\rangle^2] \\ & + \max[\sum_k (\langle \widetilde{G_k^A} \otimes \widetilde{G_k^B}\rangle - \langle \widetilde{G_k^A} \otimes I\rangle\langle I \otimes \widetilde{G_k^B}\rangle)] \\ =\ & \frac{1}{2}(\mathrm{Tr}\rho_A^2 + \mathrm{Tr}\rho_B^2) + \max \sum_k \sum_{lm} U_{kl}V_{km}\tau_{lm} \\ =\ & \frac{1}{2}(\mathrm{Tr}\rho_A^2 + \mathrm{Tr}\rho_B^2) + \max \sum_k [U\tau V^T]_{kk} \\ =\ & \frac{1}{2}(\mathrm{Tr}\rho_A^2 + \mathrm{Tr}\rho_B^2) + \sum_k \sigma_k(\tau). \end{aligned} \quad (13)$$

In other words, $\min\mathcal{F}(\rho) = 1 - \sum_k \sigma_k(\tau) - (\mathrm{Tr}\rho_A^2 + \mathrm{Tr}\rho_B^2)/2$. □

*Example.–* Bennett *et al.* introduced a $3 \times 3$ bound entangled state constructed from unextendible product bases in Ref. [30]:

$$\begin{aligned} |\psi_0\rangle &= \frac{1}{\sqrt{2}}|0\rangle(|0\rangle - |1\rangle),\ |\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|2\rangle, \\ |\psi_2\rangle &= \frac{1}{\sqrt{2}}|2\rangle(|1\rangle - |2\rangle),\ |\psi_3\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)|0\rangle, \\ |\psi_4\rangle &= \frac{1}{3}(|0\rangle + |1\rangle + |2\rangle)(|0\rangle + |1\rangle + |2\rangle), \end{aligned}$$

$$\rho = \frac{1}{4}(I - \sum_{i=0}^{4} |\psi_i\rangle\langle\psi_i|). \quad (14)$$

Let us consider a mixture of this state with white noise,

$$\rho(p) = p\rho + (1-p)\frac{I}{9}. \quad (15)$$

Using the realignment criterion, one finds that the state $\rho(p)$ still has entanglement when $p > 0.8897$. In Ref. [26], it is found that the state $\rho(p)$ must be entangled for $p > p_{lur} = 0.8885$ using the nonlinear witness Eq. (4) (but not the optimal one). According to Theorem 2, one can obtain an optimal witness of Eq. (4) and find that when $p > p_{opt} = 0.8822$ the state is still entangled. Obviously, the optimal witness is stronger than the one in Ref. [26]. In addition, in Sec. III we will present a lower bound on I-concurrence for the state based on Theorem 2 (see Fig. 1). From the figure, it is worth noticing that the bound is positive when $p > p_{opt} = 0.8822$.

## III. APPLICATIONS

In this section, the optimal nonlinear witnesses of pure bipartite states will be obtained using Theorem 2. Moreover, we will show a lower bound on the I-concurrence of bipartite systems by means of our method. Before embarking on our investigation, we first define that $\mathcal{L} = \frac{1}{2}\sum_k \langle G_k^A \otimes I - I \otimes G_k^B\rangle^2 + \sum_k \langle G_k^A \otimes G_k^B\rangle$, and obviously $\mathcal{L}_{max} = \sum_k \sigma_k(\tau) + (\mathrm{Tr}\rho_A^2 + \mathrm{Tr}\rho_B^2)/2$ according to Theorem 2.

### A. Optimal witnesses of bipartite pure states

Let us calculate $\mathcal{L}_{max}$ of a bipartite pure state $|\psi\rangle$ with its Schmidt decomposition $|\psi\rangle = \sum_i \sqrt{\mu_i}|ii\rangle$.

Since Schmidt decomposition of a pure state is a LU transformation, $\mathcal{L}_{max}(|\psi\rangle)$ remains invariant after the transformation according to Lemma 1. Therefore, we can directly use the Schmidt decomposition form for convenience. We choose a complete set of LOOs Eq. (11) and Eq. (12) for A and B subsystems, respectively (obviously any other complete set of LOOs can be chosen and it does not affect the final result).

According to Theorem 2,

$$\begin{aligned}\tau_{lm} &= \langle G_l^A \otimes G_m^B\rangle - \langle G_l^A \otimes I\rangle\langle I \otimes G_m^B\rangle \\ &= [D \oplus D \oplus T]_{lm}, \end{aligned} \quad (16)$$

where $D = diag\{\sqrt{\mu_1\mu_2}, \cdots, \sqrt{\mu_m\mu_n}\cdots, \sqrt{\mu_{d-1}\mu_d}\}$ and

$$T = \begin{pmatrix} \mu_1 - \mu_1^2 & -\mu_1\mu_2 & \cdots & -\mu_1\mu_d \\ -\mu_1\mu_2 & \mu_2 - \mu_2^2 & \cdots & -\mu_2\mu_d \\ \vdots & \vdots & \ddots & \vdots \\ -\mu_1\mu_d & -\mu_2\mu_d & \cdots & \mu_d - \mu_d^2 \end{pmatrix}. \quad (17)$$

Therefore,

$$\sum_k \sigma_k(\tau) = 2\sum_{m<n}\sqrt{\mu_m\mu_n} + 2\sum_{m<n}\mu_m\mu_n, \quad (18)$$

$$\frac{1}{2}(\mathrm{Tr}\rho_A^2 + \mathrm{Tr}\rho_B^2) = \sum_i \mu_i^2, \quad (19)$$

$$\mathcal{L}_{max}(|\psi\rangle) = (\sum_i \sqrt{\mu_i})^2. \quad (20)$$

Note that Eq. (20) has also been derived with another totally different method in Ref. [23], and it completely accords with our result. Compared with the method in Ref. [23], Theorem 2 in this paper is more general, i.e., it suits not only bipartite pure states but also any bipartite mixed state.

### B. Lower bound on the I-concurrence

I-concurrence of a bipartite pure state is given by $C(|\psi\rangle) = \sqrt{2(1-\mathrm{Tr}\rho_A^2)}$, where the reduced density matrix $\rho_A$ is obtained by tracing over the subsystem B. It can be extended to mixed states $\rho$ by the convex roof,

$$C(\rho) = \inf_{\{p_i, |\psi_i\rangle\}} \sum_i p_i C(|\psi_i\rangle),\ \rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \quad (21)$$

for all possible decomposition into pure states, where $p_i \geq 0$ and $\sum_i p_i = 1$.

Several bounds have already been derived [21, 22, 23, 24], e.g., an analytical lower bound based on PPT criterion and the realignment criterion has been shown by Chen *et al.*,

$$C(\rho) \geq \sqrt{\frac{2}{m(m-1)}}(\max(\|\rho^{T_A}\|, \|\mathcal{R}(\rho)\|) - 1), \quad (22)$$

where $T_A$, $\mathcal{R}$ and $\|\cdot\|$ stand for partial transpose, realignment and the trace norm (i.e. the sum of the singular values), respectively. In Ref. [23], another bound based on LOOs has been obtained, which has used Eq. (20) and the fact that $\sum_i p_i \mathcal{L}_{max}(|\psi_i\rangle) \geq \sum_i p_i \mathcal{L}(|\psi_i\rangle) \geq \mathcal{L}(\sum_i p_i |\psi_i\rangle\langle\psi_i|)$, (for convenience, the lower bound has been rewritten in an equivalent form)

$$C(\rho) \geq \sqrt{\frac{2}{m(m-1)}}(\mathcal{L} - 1). \quad (23)$$

Notice that Eq. (23) holds for arbitrary set of LOOs, including the optimal one. Therefore, a tighter form of Eq. (23) can be obtained according to Theorem 2,

$$C(\rho) \geq \sqrt{\frac{2}{m(m-1)}}(\mathcal{L}_{max} - 1), \quad (24)$$

where $\mathcal{L}_{max} = \sum_k \sigma_k(\tau) + (\mathrm{Tr}\rho_A^2 + \mathrm{Tr}\rho_B^2)/2$. Since the entanglement criteria based on LURs are strictly stronger

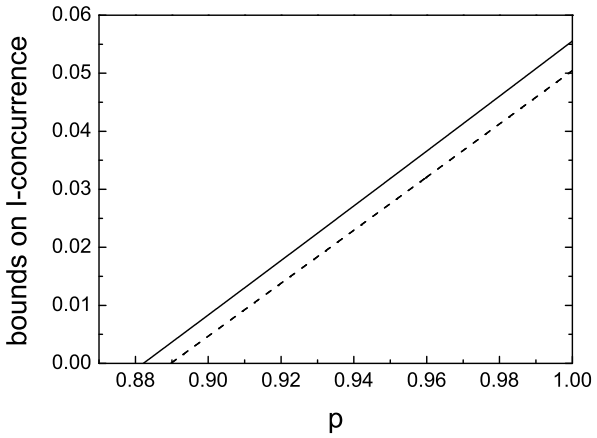


FIG. 1: Two lower bounds of I-concurrence for the state $\rho(p)$. One is the lower bound based on realignment criterion (dashed line), the other is obtained from $\mathcal{L}_{max}$ (solid line).

than the realignment criterion [26], the following inequality can be concluded.

$$C(\rho) \geq \sqrt{\frac{2}{m(m-1)}}(\max(\|\rho^{T_A}\|, \mathcal{L}_{max}(\rho)) - 1). \quad (25)$$

For example, reconsider the bound entangled state Eq. (14). Because it belongs to PPT entangled state, the lower bound based on PPT criterion is unhelpful. One can obtain that $C(\rho) \geq 0.050$ via the realignment criterion, and $C(\rho) \geq 0.052$ has been gotten in Ref. [23] by using Eq. (23). In fact, $\mathcal{L}_{max}(\rho)$ can be directly calculated, and it suggests that $C(\rho) \geq 0.055$ via Eq. (24), which is better than the one in Ref. [23]. Furthermore, one can consider the bound entangled state with white noise, i.e. Eq. (15). The lower bounds of I-concurrence for $\rho(p)$ have been shown in Fig. 1. Therefore, the lower bound based on $\mathcal{L}_{max}$ has been strictly improved compared with the one based on the realignment criterion and provided a tighter form of Eq. (23).

## IV. DISCUSSION AND CONCLUSION

During the last two sections, we consider a simple situation: the $d \times d$ bipartite system for convenience. However, if the dimensions of the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ are not the same, what will happen? Actually, it does not affect any one of the conclusions in Sec. II and Sec. III.

Without loss of generality, suppose that $m = \dim(\mathcal{H}_A) < n = \dim(\mathcal{H}_B)$. There are $m^2$ elements in a complete set of LOOs $\{G_k^A\}$, and $n^2$ elements in $\{G_k^B\}$. Therefore, we need to reconsider Eq. (8) and Eq. (13) in Theorem 1 and Theorem 2, respectively.

$$\max \sum_k \sum_{lm} U_{kl} V_{km} \mu_{lm} = \max \mathrm{Tr}(U \mu V^T), \quad (26)$$

$$\max \sum_k \sum_{lm} U_{kl} V_{km} \tau_{lm} = \max \mathrm{Tr}(U \tau V^T), \quad (27)$$

where $U$ is an $m^2 \times m^2$ real orthogonal matrix; $\mu$ and $\tau$ are $m^2 \times n^2$ real matrices; $V$ belongs to $n^2 \times n^2$ real orthogonal matrices. The two equations have the same form, so we just need to consider Eq. (27) for instance.

As Ref. [26] did, one can define that $G_k^A = 0$ for $k = m^2 + 1, \cdots, n^2$. Thus, the matrix $\tau$ is changed into an $n^2 \times n^2$ real matrix, i.e.,

$$\tau' = \begin{pmatrix} \tau \\ 0 \end{pmatrix}, \quad (28)$$

where 0 stands for an $(n^2 - m^2) \times n^2$ matrix with every element being equal to 0.

Define that $U' = U \oplus I$, where $I$ is an $(n^2 - m^2) \times (n^2 - m^2)$ identity matrix. It is easy to see that $U'$ is an $n^2 \times n^2$ real orthogonal matrix since $U$ belongs to $m^2 \times m^2$ real orthogonal matrices.

Notice that $(l \equiv n^2 - m^2)$

$$\begin{pmatrix} U_{m^2 \times m^2} & 0 \\ 0 & I_{l \times l} \end{pmatrix} \begin{pmatrix} \tau_{m^2 \times n^2} \\ 0_{l \times n^2} \end{pmatrix} \left( V^T_{n^2 \times n^2} \right) = \begin{pmatrix} [U \tau V^T]_{m^2 \times n^2} \\ 0_{l \times n^2} \end{pmatrix},$$

which means that $\mathrm{Tr}[U' \tau' V^T] = \mathrm{Tr}[U \tau V^T]$. Therefore,

$$\begin{aligned} \max \mathrm{Tr}[U \tau V^T] &= \max \mathrm{Tr}[U' \tau' V^T] \\ &= \max \mathrm{Tr}[\tau' V^T U'] \\ &= \sum_k \sigma_k(\tau'). \end{aligned} \quad (29)$$

Since $\tau' \tau'^T = [\tau \tau^T] \oplus 0_{l \times l}$, $\tau' \tau'^T$ and $\tau \tau^T$ have the same nonzero eigenvalues. Hence,

$$\sum_k \sigma_k(\tau') = \sum_k \sigma_k(\tau). \quad (30)$$

Consequently, Eq. (29) and Eq. (30) suggest that Theorem 1 and Theorem 2 still hold even if the dimensions of subsystems A and B are not the same, and the applications in Sec. III which have used the Theorem 2 can also be extended to this case.

In conclusion, we have optimized the linear and the nonlinear entanglement witnesses based on local orthogonal observables, which are introduced by Yu, Liu and Gühne *et al.* respectively, and several examples have been given as well. Moreover, we have obtained the optimal witnesses based on LOOs in pure bipartite systems and a lower bound on the I-concurrence of bipartite systems as applications of our method. In fact, Theorem 2 presents a separability criterion with Ky Fan norm of $\tau$, the covariance term defined in [27]. Similarly, another separability criterion with Ky Fan norm of correlation matrix has been shown in [31]. It is worth investigating

deeper relation between this two criterions. In addition, the 'optimal' in this paper is in the sense of choosing the best complete set of LOOs such that the witness gets its minimum, which has little relation with traditional optimal EWs [32].

*Note added.* Recently a similar result has been shown in [33], which is based on covariance matrix criterion. Interestingly, Proposition 3 in [33] can be optimized to a similar form as Theorem 2 in this paper.

## ACKNOWLEDGMENTS

This work was funded by the National Fundamental Research Program (2006CB921900), the National Natural Science Foundation of China (10674127, 60121503), the Innovation Funds from the Chinese Academy of Sciences, and Program for New Century Excellent Talents in University.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[2] *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation and Quantum Computation*, edited by D. Bouwmeester, A. Ekert, and A. Zeilinger (Springer, New York, 2000).
[3] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[4] D. Bruß, J. Math. Phys. **43**, 4237 (2002).
[5] M. B. Plenio, S. Virmani, Quantum Inf. Comput. **7**, 1 (2007).
[6] R. Horodecki, P. Horodecki, M. Horodecki and K. Horodecki, preprint quant-ph/0702225.
[7] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[8] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
[9] O. Rudolph, preprint quant-ph/0202121; K. Chen and L.-A. Wu, Quantum Inf. Comput. **3**, 193 (2003).
[10] B. Terhal, Phys. Lett. A **271**, 319 (2000); G. Tóth and O. Gühne, Phys. Rev. Lett. **94**, 060501 (2005); M.A. Jafarizadeh, M. Rezaee, S. K. A. Seyed Yagoobi, Phys. Rev. A **72**, 062106 (2005).
[11] H. F. Hofmann and S. Takeuchi, Phys. Rev. A **68**, 032103 (2003); H. F. Hofmann, *ibid.* **68**, 034307 (2003).
[12] O. Gühne, Phys. Rev. Lett. **92**, 117903 (2004).
[13] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).
[14] J. Clauser, M. Horne, A. Shimony, and R. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[15] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990); M. Ardehali, Phys. Rev. A **46**, 5375 (1992); A. V. Belinskii and D. N. Klyshko, Phys. Usp. **36**, 653 (1993); N. Gisin and H. Bechmann-Pasquinucci, Phys. Lett. A **246**, 1 (1998).
[16] O. Gühne and N. Lütkenhaus, Phys. Rev. Lett. **96**, 170502 (2006).
[17] F. A. Bovino, G. Castagnoli, A. Ekert, P. Horodecki, C. M. Alves and A. V. Sergienko, Phys. Rev. Lett. **95**, 240407 (2005); R. Augusiak, P. Horodecki, M. Demianowicz, preprint quant-ph/0604109.
[18] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).
[19] A. Uhlmann, Phys. Rev. A **62**, 032307 (2000).
[20] P. Rungta, V. Bužek, C. M. Caves, M. Hillery and G. J. Milburn, Phys. Rev. A **64**, 042315 (2001).
[21] F. Mintert, M. Kuś and A. Buchleitner, Phys. Rev. Lett. **92**, 167902 (2004).
[22] K. Chen, S. Albeverio and S.-M. Fei, Phys. Rev. Lett. **95**, 040504 (2005).
[23] J.I. de Vicente, Phys. Rev. A **75**, 052320 (2007).
[24] H. P. Breuer, J. Phys. A: Math. Gen. **39**, 11847 (2006).
[25] S. Yu and N.-L. Liu, Phys. Rev. Lett. **95**, 150504 (2005).
[26] O. Gühne, M. Mechler, G. Tóth and P. Adam, Phys. Rev. A **74**, 010301 (R) (2006).
[27] C. Kothe and G. Björk, Phys. Rev. A **75**, 012336 (2007); Z.-W. Wang, Y.-F. Huang, X.-F. Ren, Y.-S. Zhang and G.-C. Guo, Europhys. Lett. **78**, 40002 (2007).
[28] Theorem 7.4.9 in R. A. Horn and C. R. Johnson, *Matrix Analysis* (Cambridge University Press, Cambridge, 1985).
[29] M. A. Nielsen, Ph.D. thesis, University of New Mexico (1998), preprint quant-ph/0011036; M. A. Nielsen, C. M. Dawson, J. L. Dodd, A. Gilchrist, D. Mortimer, T. J. Osborne, M. J. Bremner, A. W. Harrow and A. Hines, Phys. Rev. A **67**, 052301 (2003).
[30] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin and B. M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999).
[31] J.I. de Vicente, Quantum Inf. Comput. **7**, 624 (2007).
[32] M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki, Phys. Rev. A **62**, 052310 (2000); M. Lewenstein, B. Kraus, P. Horodecki, and J. I. Cirac, *ibid.* **63**, 044304 (2001).
[33] See Proposition 3 in O. Gühne, P. Hyllus, O. Gittsovich, and J. Eisert, preprint quant-ph/0611282v2.